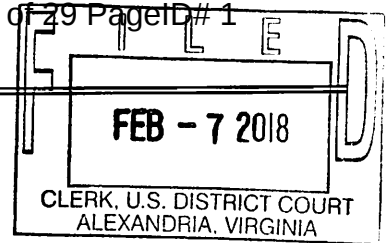


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

THE PREMISES LOCATED AT
6400 BLARNEY STONE COURT
SPRINGFIELD, VA 22152-2129

Case No. 1:18-SW-74

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 2252 and 2252A Possessing, receiving, or distributing child pornography.

The application is based on these facts:

See attached affidavit.

- ☐ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher P. Schmaltz, Special Agent, USACIDC

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/07/2018City and state: Alexandria, Virginia

/s/

Ivan D. Davis

United States Magistrate Judge

ATTACHMENT A

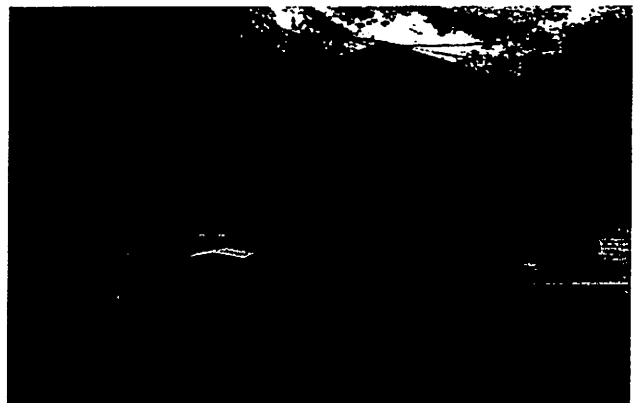
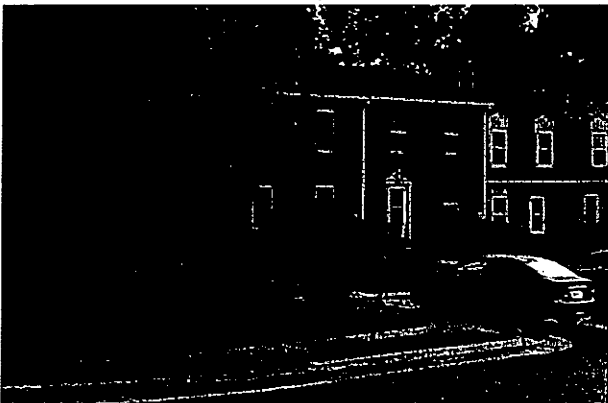
PREMISES TO BE SEARCHED

The premises to be searched are the entire premises located at 6400 Blarney Stone Court, Springfield, VA 22152-2129, hereinafter the SUBJECT PREMISES. The SUBJECT PREMISES is more fully described as a two-story townhome with a brick façade and vinyl shutters. The premises to be searched includes any appurtenances to the real property that is the SUBJECT PREMISES and any storage units/outbuildings. Due to the ability and ease for individuals to upload and save child pornography onto media storage devices such as CDs, DVDs, and thumb drives, which can be easily concealed and stored inside of a vehicle, the premises to be searched includes vehicles on the SUBJECT PREMISES that are owned by Marc Kodack, owner of the SUBJECT PREMISES.

A birds-eye view photograph of the SUBJECT PREMISES is below:



Photographs of the SUBJECT PREMISES' exterior (front and west side) are below:



ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

Contraband, fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Sections 2252 and 2252A (activities relating to child pornography), including:

1. Child pornography and images or visual depictions of minors engaged in sexually explicit conduct;
2. Child erotica;
3. Information, correspondence, records, documents or other materials, including computers, mobile phones, or storage media, constituting evidence of or pertaining to the production, possession, receipt, distribution, accessing with intent to view, or transmission through interstate or foreign commerce of items “1” and “2” above, or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children;
4. For any computer, mobile phone or storage medium whose seizure is authorized by this authorization, and any image of such computer, mobile phone or storage medium (hereinafter, “COMPUTER”):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this search and seizure authorization were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

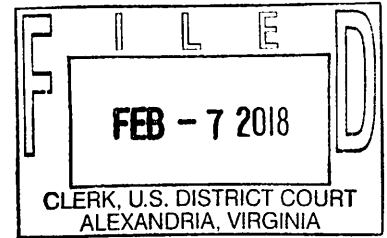
As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer,” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium,” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, DVDs, and other magnetic, electronic, or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT
6400 BLARNEY STONE COURT,
SPRINGFIELD, VA 22152-2129

Case No. 1:18-sw-74

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Christopher P. Schmaltz, being first duly sworn, hereby depose and state that the following is true to the best of my information, knowledge and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for the premises at 6400 Blarney Stone Court, Springfield, VA 22152-2129 (SUBJECT PREMISES), to seize evidence described in Attachment A, and to search any seized evidence for items that constitute the commission of, contraband, the fruits of crime, or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, Distribution and Possession of Child Pornography.

2. I am a Special Agent of the Computer Crime Investigative Unit (CCIU), United States Army Criminal Investigation Command (USACIDC/CID), and have been so as an active Army or Army Reserve service member since 2006. I have approximately 11 years of law enforcement experience with Army CID. Prior to my position with CCIU, I was employed as a contract Digital Forensic Analyst with Booz Allen Hamilton at Army Cyber Command in Fort Belvoir, VA. My formal education includes a Master's Degree in High Technology Crime

Investigation from the George Washington University and a Bachelor's Degree in International Relations from The University of Minnesota. In addition to my training as a Criminal Investigator, I have been trained in Computer Networks and Hardware, Computer Incident Response, Windows Forensic Examinations at the Department of Defense Cyber Investigations Training Academy (DCITA) and have been certified as a Digital Forensic Examiner (DFE) through DCITA. My other technical certifications include: Certified Ethical Hacker (CEH) through EC Council, Network+ and Security+ through CompTIA. My duties at CCIU include the investigation of crimes involving computer-related offenses including computer intrusions and other types of malicious computer activity directed against the U.S. Army or conducted using Army computers. Also as part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A. I have received training and instruction in child pornography investigations and have conducted investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet and printed images).

3. This affidavit is submitted in support of an application for a search warrant for records of suspected child pornography. This information is likely stored in records and electronic storage mediums, including previously collected USB digital devices that were forensically imaged by the CCIU with the consent of Marc Kodack. As described in further detail below, when at the residence of Marc Kodack on or about December 19, 2017, your Affiant observed in plain view that the aforementioned collected USB digital devices were

connected to computers at the SUBJECT PREMISES. As also described in more detail below, forensic examinations of the images of these USB digital devices revealed that they contained suspected child pornography, and that they contained file back-ups for other computers. Consequently I submit that there is probable cause to believe that located in the SUBJECT PREMISES are items as described in Attachment B containing evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a) and 2252A(a).

4. Because this affidavit is being submitted for the limited purpose of securing a search and seizure warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a) and 2252A(a) are located in the place described in Attachment A.

5. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.

RELEVANT STATUTES

6. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing child pornography with the intent to view it as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility

or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit activity (that is, child pornography).

PROBABLE CAUSE

I. Background

7. On October 8, 2017, a security system product on the government laptop used by Department of Army employee Marc Kodack, a Program Manager with the Assistant Secretary of the Army, Installations, Energy and Environment (ASA IE&E), executed an automated virus scan on that laptop after a peripheral USB digital device was connected to the system. A USB digital device is a device that uses a common connection platform to enable a computer to interface with the device. This is typically used by electronic storage mediums for retention of digital information on a hard drive. The scan resulted in an alert to the Pentagon Computer Incident Response Team (PENTCIRT) when it showed the connected USB digital device contained a malicious file.

8. PENTCIRT is a unit located in the Pentagon that analyzes systems across the Department of Defense enterprise when security systems indicate alerts of compromise, malware infection, or other security violations. According to Army policy, such a security violation includes connecting unauthorized devices, which could introduce malicious software onto a system. Because the security alert described in Paragraph 7 indicated that an unauthorized USB digital device containing potential malware was connected to an Army computer, PENTCIRT requested that ASA IE&E's IT administrators obtain Kodack's government laptop for examination.

9. On October 17, 2017, PENTCIRT received Kodack's government laptop from the ASA IE&E IT administrators, and a forensic image of the system was created. The government laptop used by Kodack displayed a standard Department of Defense login banner which articulated that use of the system constituted consent to monitoring for network defense or law enforcement purposes. PENTCIRT subsequently performed a forensic examination of the image, which determined that from October 6 through 15, 2017, USB digital devices were connected to Kodack's government laptop. The security system product on the government laptop indexed the contents of the connected USB digital devices showing, what appeared to be, back-ups of Kodack's personal computer. A "back-up" is a file usually created through an automated saving process which creates a copy of a user's computer system, with updated changes made since the last previous back-up. The back-ups in this case, according to security system logs on the government laptop, were shown to also contain malware.

10. In addition to malware, PENTCIRT's examination found on Kodack's government laptop approximately 645 indexed images from a USB digital device that had previously been connected to it. Some of the images showed individuals engaged in sexual intercourse with animals, and other images depicted unclothed girls. A review of all images identified six thumbnail images of prepubescent females, approximately 10 – 12 years of age, nude on a beach like setting. Although the girls were nude, some covered only in body paint, the images did not focus on genitalia, nor were they explicit depictions of sexual conduct.

11. On November 6, 2017, your Affiant and another Agent of CCIU met with the PENTCIRT's forensic examiner, who provided his examination results.

12. The hard drive of Kodack's government laptop was taken from PENTCIRT and imaged for analysis by CCIU's Digital Forensic Research Branch (DFRB). On December 18, 2017, DFRB's examination confirmed that the security system on Kodack's government system logged malicious files which were on a connected USB digital device. Coinciding with this connection, event logs showed Kodack's user profile was signed onto the government laptop.

II. Interview and Consent to Search

13. On December 19, 2017, a voluntary, non-custodial interview of Kodack was conducted by three Agents at the Pentagon: your Affiant, and another CCIU and a Pentagon Force Protection Agent (PFPA) Agent. During the interview, Kodack stated that he connected a personally owned external hard drive to his government laptop. He stated that his connected USB digital device contained Windows 10 back-ups for his personal computer. Furthermore, Kodack stated he would consent to have his personal USB digital devices forensically imaged to be analyzed for malware.

14. After the interview, Kodack agreed to accompany your Affiant and a CCIU Agent to his residence at the SUBJECT PREMISES. The SUBJECT PREMISES is a two-story town-home with Kodack as the single occupant. While there, Kodack escorted CCIU Agents to a bedroom on the second story of the home. This bedroom appeared to function as an office space with a desk that had two computers, an HP model desktop workstation, and a Dell All-in-One model computer, which is a computer with an integrated monitor. Your Affiant observed that each computer had USB digital devices attached to it. Kodack signed a form for Consent to Search for malware and voluntarily gave 7 external hard drives and a USB thumb drive to your Affiant. To date, Kodack has not revoked his consent. At the time, Kodack stated to Agents

although he would release the USB digital devices to CCIU, he did not wish to provide the computers – that is, the HP desktop and Dell computer – to CCIU for imaging.

15. On December 19, 2017, your Affiant started to process forensic images of Kodack's USB digital devices. On December 20, 2017, the processing of forensic images of Kodack's personal USB digital devices was completed by CCIU, and verified and documented by your Affiant. The images of Kodack's USB digital devices were stored onto a hard drive and temporarily stored in an evidence locker at Quantico, VA. The same day, the 7 external hard drives and USB thumb drive were returned to Kodack at the SUBJECT PREMISES by your Affiant and another CCIU Agent.

16. On December 22, 2017, the hard drive containing the forensic images obtained from Kodack's personal USB digital devices was turned into the CCIU Evidence Room in Quantico, VA to the assigned evidence custodian. A subsequent request to examine the images of the USB digital devices for malware was submitted by your Affiant to CCIU DFRB.

III. Forensic Analysis and Discovery

17. On December 27, 2017, an Agent of CCIU DFRB conducted an examination of one of the forensic images of Kodack's USB digital devices, a backup of a Windows 10 system, using the Magnet Forensics Axiom examination tool. As part of his normal processing of evidence, the DFRB Agent executed parsing tools which included Project VIC hash sets. Based on my training and experience, I know that Project VIC is a network of law enforcement and private sector partners who collect the digital hash values of known child pornographic material. These hashes are provided to law enforcement in sets for later identification in digital forensic examinations. Upon previewing Google searches to determine whether Kodack had researched

computer viruses or if his search history indicated that his system had been previously impacted by malware, the first Google search result that appeared stated “Preteen nude girls sex.” The Agent then checked the Project VIC hash sets which revealed numerous hits. Checking these results the Agent observed a series of images, the first of which displayed two Caucasian, prepubescent females, totally nude. One of the minor females was facing the camera on her knees and elbows, while the other was reclined over her. The reclining girl was posed with her legs spread wide open, exposing her vagina to the camera.

18. Upon seeing this image, the DFRB Agent terminated his examination and contacted your Affiant and another CCIU Agent, who both also observed the image and confirmed that it was suspected child pornography as defined by Title 18, United States Code, section 2256.

III. Search and Seizure Warrant and Examination

19. On January 24, 2018, your Affiant swore to an affidavit containing the general information provided in paragraphs 7 – 18 above, and pursuant to Federal Rule of Criminal Procedure 41(b)(1), a search and seizure warrant was obtained from the United States District Court for the Eastern District of Virginia that authorized the examination of the forensic images of Kodack’s USB digital devices for child pornography.

20. Pursuant to the search and seizure warrant referenced in paragraph 19 above, on January 25, 2018, an Agent of CCIU DFRB examined the forensic images of Kodack’s USB digital devices for child pornographic material. Using the Magnet Forensics Axion examination tool, the DFRB Agent’s preliminary examination has found contained in one of these images was a Windows 10 backup of a Windows 10 virtual machine, which contained 360

visual depictions of child erotica and suspected child pornography. The visual depictions were located in the same forensic image of Marc Kodack's USB digital device analyzed in paragraph 17.

21. The child erotica and suspected child pornography files were located in the database file known as Thumbs.db. The Thumbs.db file is a cache file, which is used by Windows 10 operating systems so that imagery can be quickly viewed by a user as a smaller image file in place of the original image. Although images in Thumbs.db files are not original images accessed and viewed by users, they are smaller resolution depictions of the original image files on the system. The Thumbs.db files are hidden files, accessed by the operating system and not viewed by most users. Even when images are deleted from a Windows 10 operating system, frequently the Thumbs.db images remain. Some of the suspected child pornographic image files reviewed in Thumbs.db are described as follows:

- a. An image depicting two Caucasian, prepubescent females, totally nude. One of the minor females was facing the camera on her knees and elbows, while the other was reclined over her. The reclining girl was posed with her legs spread wide open, exposing her vagina to the camera.
- b. An image depicting a black, prepubescent female, under 10 years of age, partially clothed in green, yellow and pink satin like stockings. Her midriff is bare and she is laying forward with her knee forward so as to display her vagina to the camera.
- c. An image of the same prepubescent female as described in paragraph 21.b., with green, yellow and pink satin stockings visible. The image is cropped as to focus on her vagina with her legs spread wide open.

- d. An image depicting a white, prepubescent female, between 10 and 12 years of age, on her knees and elbows with her head turned over her shoulder looking towards the camera. There is a decorative yellow and red arm-band on her left arm. Her vagina is the central focus of the image.

22. Your Affiant coordinated with CCIU's Liaison to Internet Crimes Against Children (ICAC) who determined through his resources at the National Center for Missing and Exploited Children (NCMEC) that of the 360 images of child erotica and child pornography found on the system, one image contained at least 1 child victim previously identified by law enforcement.

23. Based on the discovery of child pornography on the forensic images of the collected USB digital devices, I submit there is probable cause to believe that a search of the SUBJECT PREMISES may yield substantive evidence in the form of child pornographic materials. This is due partly due to the ease in which the USB digital connection platform enables and facilitates the transfer of data between computers and other electronic systems. Any USB electronic storage medium stands as a potential container or device for the transfer of contraband material.

24. Due to the ability and ease for individuals to upload and save child pornography onto media storage devices such as CDs, DVDs, and thumb drives, which can be easily concealed and stored inside of a vehicle, this warrant application seeks authorization to search vehicles on the SUBJECT PREMISES that are owned by Kodack, owner of the SUBJECT PREMISES, for such media devices.

25. Furthermore, your Affiant respectfully requests permission to search and seize images and videos of child pornography, including those that may be stored on computers or electronic storage mediums. These things constitute both evidence of a crime and contraband. This affidavit also requests permission to seize the computer hardware and electronic storage mediums that may contain those things if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In this case, computer hardware that was used to store child pornography is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.

26. LexisNexis, CLEAR, and TLO are database resources commonly used by Law Enforcement for background information on subjects in criminal investigations. Each of these reports indicates Kodack owns and resides at the SUBJECT PREMISES.

COLLECTORS OF CHILD PORNOGRAPHIC MATERIAL

27. Based upon my training and experience in child sexual exploitation and child pornography investigations, and having worked with other experienced law enforcement officers in child exploitation investigations, I know the following:

- a. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of illicit materials from discovery, theft, and damage. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit

materials with passwords, encryption, and other security measures. These individuals may also protect their illicit materials by saving them on movable media such as memory cards, memory sticks, CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be easily secreted as they are very small in size - often as small as a postage stamp - or sent to third party image storage sites via the Internet.

- b. Individuals who maintain images of child pornography often maintain these images on cameras, film, video cameras, videos, computers, and other photographic equipment.
- c. Individuals who collect child pornography will frequently conceal their digital media devices on their person so as to conceal their activities from family members and protect their digital content. These individuals may also store the information in their mobile telephone to allow remote access to their collections while travelling. Media storage devices are frequently marketed for their portability and can come in various shapes and sizes to include key chains, sunglasses, or toys.
- d. Another frequent location for the storage of portable media devices is within a vehicle controlled by the suspect. Previous searches of vehicles by law enforcement in similar investigations have revealed thumb drives, mobile phones, laptop computers, cameras, and SD Cards stored within vehicle compartments.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- b. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, mobile telephones, video gaming devices, portable electronic music players, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- c. “Digital Device,” as used herein, is defined as any electronic device capable of processing and/or storing data in digital form, including, but not limited to: central processing units, laptop or notebook computers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, cables and connections, electronic storage media, electronic/digital security devices, and

wireless communication devices such as telephone paging devices, beepers, mobile or cellular telephones, “smart” watches, personal data assistants (“PDAs”), iPods, BlackBerrys, digital cameras and digital gaming devices.

- d. “Downloading” is the process of transferring a file from the Internet and saving it as a file in one's computer hard drive.
- e. “Uploading” is the process of transferring a file from one's computer to the computer of another user via the Internet.
- f. “Hashing” is a powerful and pervasive technique used in nearly every examination of seized digital media. The concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data. Examiners use hash values throughout the forensics process, from acquiring the data, through analysis, and even into legal proceedings. Hash algorithms are used to confirm that when a copy of data is made (commonly referred to as a forensically sound image, the original is unaltered and the copy is identical, bit-for-bit.” A hash value can be thought of as a digital fingerprint of the information.
- g. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical,

electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- h. A “storage medium” is any physical object upon which computer data can be recorded. Examples include CD-ROMs, DVDs, and other magnetic or optical media.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. There is probable cause to believe that things that were once stored on the a device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a

computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the digital device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the digital devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the forensic images consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

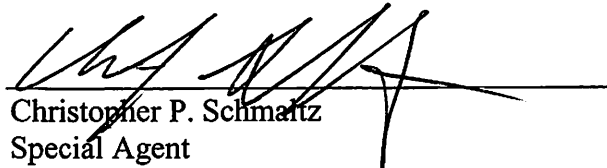
33. *Manner of execution.* In light of these concerns, I hereby request permission to seize any records, electronic storage mediums, and computer hardware (including associated peripheral USB digital devices which were imaged with consent) that are believed to contain some or all of the evidence described in the authorization, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

34. Searching computer systems for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the authorization. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the authorization. In light of these difficulties, CCIU intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.


CONCLUSION

35. I submit that this affidavit supports probable cause for a search warrant to search the SUBJECT PREMISES described in Attachment A for the things described therein and a subsequent search of the seized items for records and information set out in Attachment B which are related to the offense also set out there, and seizure of those records and information.

Respectfully submitted,


Christopher P. Schmalz
Special Agent
USACIDC

Subscribed and sworn to before me on February 7th, 2018

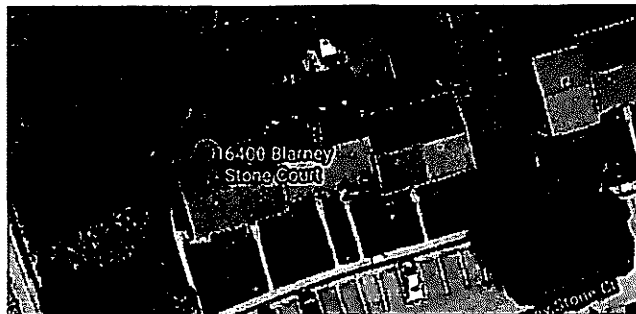
 /s/ _____
Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

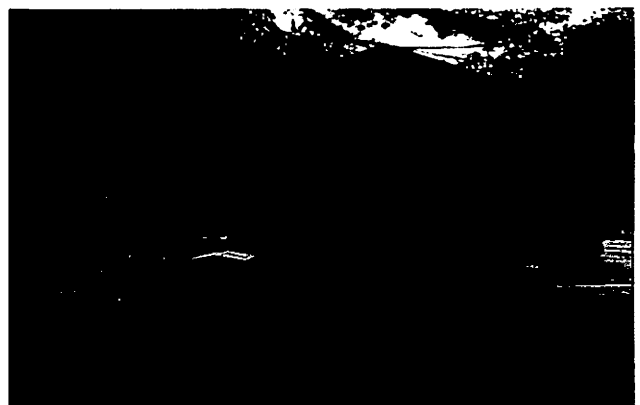
PREMISES TO BE SEARCHED

The premises to be searched are the entire premises located at 6400 Blarney Stone Court, Springfield, VA 22152-2129, hereinafter the SUBJECT PREMISES. The SUBJECT PREMISES is more fully described as a two-story townhome with a brick façade and vinyl shutters. The premises to be searched includes any appurtenances to the real property that is the SUBJECT PREMISES and any storage units/outbuildings. Due to the ability and ease for individuals to upload and save child pornography onto media storage devices such as CDs, DVDs, and thumb drives, which can be easily concealed and stored inside of a vehicle, the premises to be searched includes vehicles on the SUBJECT PREMISES that are owned by Marc Kodack, owner of the SUBJECT PREMISES.

A birds-eye view photograph of the SUBJECT PREMISES is below:



Photographs of the SUBJECT PREMISES' exterior (front and west side) are below:



ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

Contraband, fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Sections 2252 and 2252A (activities relating to child pornography), including:

1. Child pornography and images or visual depictions of minors engaged in sexually explicit conduct;
2. Child erotica;
3. Information, correspondence, records, documents or other materials, including computers, mobile phones, or storage media, constituting evidence of or pertaining to the production, possession, receipt, distribution, accessing with intent to view, or transmission through interstate or foreign commerce of items “1” and “2” above, or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children;
4. For any computer, mobile phone or storage medium whose seizure is authorized by this authorization, and any image of such computer, mobile phone or storage medium (hereinafter, “COMPUTER”):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this search and seizure authorization were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer,” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium,” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, DVDs, and other magnetic, electronic, or optical media.